A Framework for the detection of Advanced Persistent Threats(APT) Using Cyber Incident Reports

RESEARCH PROPOSAL

Nadeem Akhtar

01-247232-020

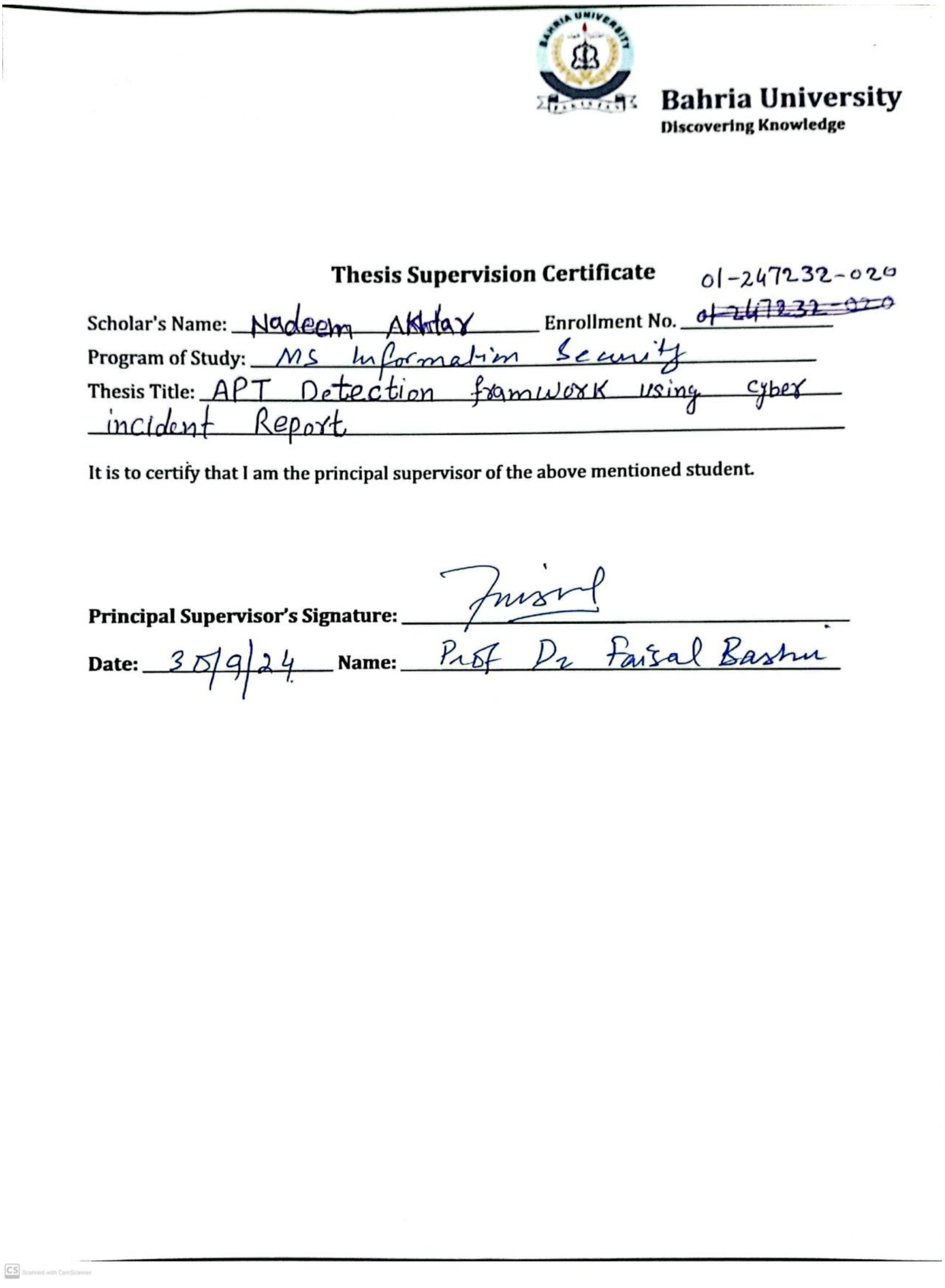
Dr Faisal Bashir

MSCS

Department of Computer Science

BAHRIA UNIVERSITY ISLAMABAD CAMPUS

Proposal Submission Certificate



Bahria University
Discovering Knowledge

Thesis Supervision Certificate

01-247232-020

Scholar's Name: Nadeem Akhtar Enrollment No. ~~01-247232-020~~

Program of Study: MS Information Security

Thesis Title: APT Detection framWORK using cyber incident Report

It is to certify that I am the principal supervisor of the above mentioned student.

Principal Supervisor's Signature: ______

Date: 30/9/24 Name: Prof Dr Faisal Bashir

TABLE OF CONTENTS

1. Introduction

In today's cyber world, preventing attacks is a challenging task. Advanced Persistent Threats (APTs) have grown their capabilities to factors that make it hard to detect and investigate security breaches. Cyberspace is an increasingly complex industry, which reflects the growing threat landscape. Today, adversaries have developed advanced tactics, techniques, and procedures (TTPs) to dynamically change their posture while evading commonplace defence mechanisms [1]. In the threat environment today, traditional cyber defence mechanisms no longer suffice. Adversary behaviours have become industry-graded and require matching advanced mechanisms by organizations to mitigate risk across their threat landscape [2] effectively. By strategically incorporating cyber threat intelligence (CTI) practices, an organization can enable itself to make proactive, informed, data-backed decisions to combat APTs. Shared threat intelligence is a vast amount of information, making it difficult for security analysts to analyze manually. The fusion of advanced technologies like ML and shared intelligence can help organizations proactively predict the current tactics used by attackers. This thesis proposes an ML approach to detect Tactics, Techniques & Procedures (TTPs) from shared threat intelligence. The proposed work evaluates different strategies hackers use to launch the most sophisticated attacks, like APTs.

After the emergence of novel threat actors, organizations cannot rely on a single solution (IDS/ IPS, SIEM). These static traditional security solutions are based on signature-based and anomaly detection, which does not match or predict new threats known to be evasive, resilient, and complex. Complex threats rely on well-advanced tactics to appear unknown to signature and anomaly detection tools yet authentic enough to bypass spam filters [5]. Today's organizations deploy a multi-layered defence to fight these threats, improving their chances of detecting or disrupting an attack. Open-Source Intelligence can provide a knowledge base to deploy multi-layered defence systems, such as anti-virus and intrusion prevention. This knowledge can be collected using threat intelligence platforms (TIPs) like MISP and OpenCTI. However, Threat Intelligence Platforms (TIPs) receive millions of security events daily. This makes it hard to analyze and extract relevant information about upcoming threats.

Similarly, Fake Cyber Threat Intelligence (FCTI) is also poisoning the threat intelligence data and making it difficult for organizations to extract more relevant and appropriate intelligence from TIPs. According to recent surveys, the volume and quality of data are the most common barriers to effective information exchange. Most organizations cannot use threat data because there are too many, approximately 250 million indicators per day [9].

In this research, we propose diverse Machine Learning approaches (Multi-Label Text classification models) to retrieve TTPs from textual sources of Cyber Threat Intelligence known as Cyber Threats Intelligence Reports (CTRs). CTRs came from the most authentic organizations like IBM X-Force, Fire-Eye, MacAfee, and Kaspersky. These reports contain the most factual and subterranean analysis of active adversaries around the globe. On the other side, fake threat intelligence from threat actors has tainted vast data, making it less credible and difficult for analysts to extract critical information. The proposed system is used in compliance with the MITRE ATT&CK framework (an open knowledge base of adversarial Tactics and techniques). It outputs TTPs in benchmark formats of STIX and TAXI standards, making it highly compatible with organizational security structures.

To provide proper cyber security risk mitigation, organizations must develop different strategies and approaches to combat the increasingly complex adversary threat field [3]. Part of the solution is utilizing CTI. FireEye defines cyber threat intelligence as follows: "Evidence-based knowledge about adversaries – their motives, intents, capabilities, enabling environments and operations – focused on an event, series of events or trends, and providing a decisive advantage to the defender." Through this definition, CTI focuses on adversaries and their behaviours due to attacks and defence actions being executed because of human interaction. This approach to defining CTI facilitates a high-level focus on the attackers themselves rather than their low-level techniques. Doing so enables organizations to implement proactive defences based on their adversary's intents and capabilities. For CTI, FireEye defines the difference between information (often not actionable) and intelligence (includes content that makes it actionable). Information, for example, might include a malicious IP address or malware hash signature. These alone may help an organization defend, but that information is too low-level to form an intelligence-driven defence posture. Intelligence includes information but has added analysis, evaluation, relation, and context. This can include how malware is used strategically, an APT's preferred set of malware tools, the types of industries and APT targets, etc.

To protect valuable assets, corporate networks are equipped with security devices such as traditional firewalls, IDS, IPS, anti-malware software, traffic sniffers, etc. These devices are rule-based detection systems that allow or reject traffic according to the rules. On the other hand, cybersecurity is a process, not a product, which needs continued monitoring and improvement. Therefore, it is essential to think of advanced cyber threat handling more analytically. Hunting potential threats are more sophisticated than a traditional rule-based detection system [4]. To detect or handle a cyber-attack, it is essential to learn about the weaknesses of the Network. It is indispensable for the cybersecurity team to understand the techniques and motive of the attacker, what data could be targeted and why the attack happened [5][6].

1.1 Cyber Threat Intelligence

While reviewing research, it became clear that threat intelligence was seen as a differentiator. Since there is so much noise, the availability of tremendous amounts of information, and a multitude of alerts, it is vital that intelligence is seen as a differentiator and is vital to filter through the noise and the abundance of information that inundates companies much time. Secondly, threat intelligence is also about classifications, that is, having the ability to classify into various categories to know which category needs focus and which does not. Some authors have discussed the importance of different phases of the intelligence lifecycle and various intelligence gathering tools that help organizations map, quantify, and enrich all the collected data surrounding the other available threats [13].

The speed of attacks is continuously increasing with no signs of slowing down. Many authors have mentioned that information overload has become prevalent, which is true in the security arena. This is considering the volume of attacks and the increase in the sophistication of attacks, including ransomware, etc. Hence, one of the biggest challenges is centring on alert overload, considering the sheer volume of alerts most organizations face. It might be challenging to understand how these interoperate, execute, or infiltrate needed data despite knowing about these threats. To move from the unknown threats to the know threats category is vital as this understanding can be used for mitigation of the threat or to deter the threat. Such classification is critical as organizations must put proactive measures to mitigate and deter the threat.

1.2 Advance Persistent Threats (APTs)

Today's generation threats are multi-vectored, i.e., most attacks use multiple means of propagation, such as social engineering, email, and application vulnerabilities, and often multistage, meaning that most attacks operate in different phases, such as single device compromise, lateral network movement and data exfiltration [10]. These complex threats rely on social engineering techniques, the latest zero-day vulnerabilities, and well-advanced tactics for appearing unknown to signature-based tools and yet authentic enough to bypass spam filters. Traditional security defences were developed to inspect each attack vector as a separate path and each stage of an attack as an independent event, failing to identify and analyze an attack as an orchestrated series of cyber incidents [11].

The advanced persistent threats (APT), being one of today's generation threats that had a significant impact on the rise of cybercrime, branched from young hackers in the "black hat" community, whose objective was to feed by states and private entities [12]. Targets are typically governments or organizations with significant intellectual property value. While traditional attacks propagate as broadly as possible to improve the chances of success, an advanced persistent threat attack only focuses on its pre-defined targets. As for the attack objectives, advanced persistent threats look for digital assets that bring competitive advantage or strategic benefits, such as intellectual property and trade secrets. In contrast, traditional threats mostly search for information that facilitates financial gain, like credit card data. The actors behind advanced persistent threats are a group of skilled hackers working in a coordinated way. They may work in a government cyber unit or be hired as cyber mercenaries by governments and private organizations. They are well-resourced from both financial and technical perspectives. This allows them to work for an extended period and access zero-day vulnerabilities and attack tools.

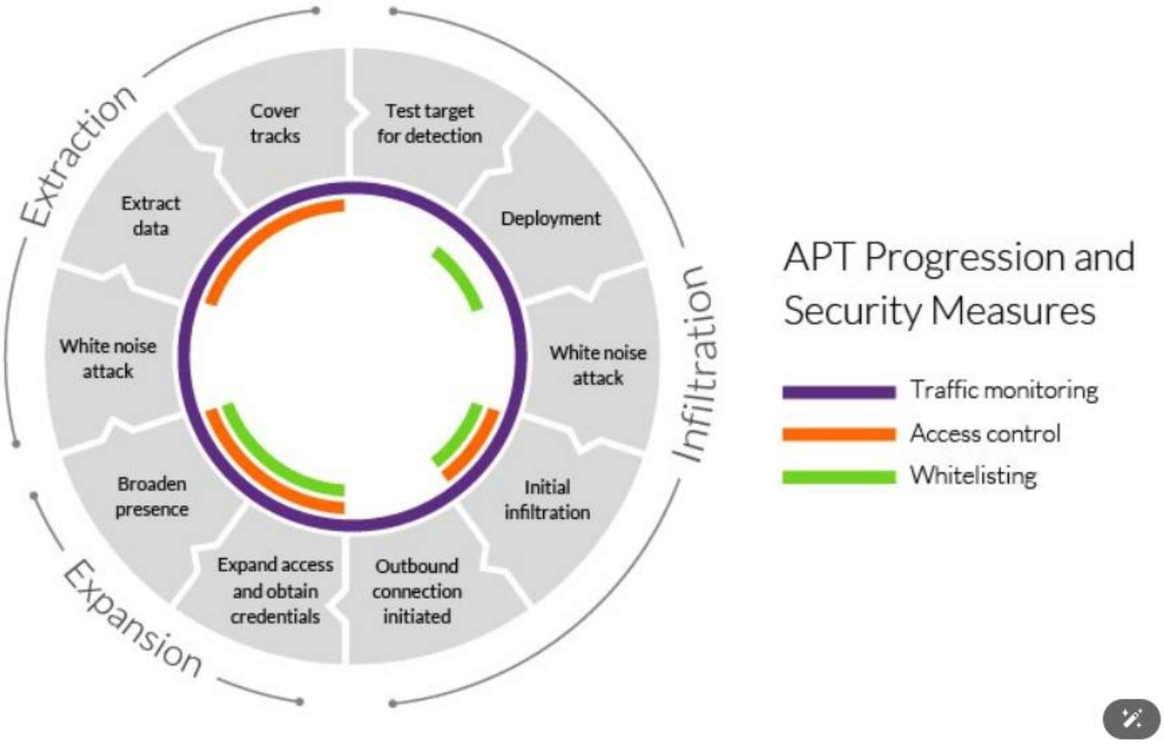


Figure:1 Advanced Persistent Threats (APT) Lifecycle

APTs have a long-term campaign, which can stay undetected in the target's Network for several months or years. Threat actors persistently attack their targets and repeatedly adapt their efforts to complete the job. Traditional attackers often target a wide range of victims and move to something less secure if they cannot penetrate the initial target. APTs attacks are stealthy, concealing within enterprise network traffic and interacting just enough to achieve the defined objectives. For example, APT actors may use encryption to obfuscate network traffic. This is different from traditional attacks, where the attackers typically employ tactics that alert the defenders. Conclusively, the APT's attacker chain can only be broken by understanding the TTPs being used by attackers.

1.3 Cyber Kill Chain

APTs can be understood from the defensive perspective of a "kill chain ."A cyber kill chain is a model that defines a sequence of stages required for an attacker to infiltrate a network and exfiltrate data from it successfully. This model provides a framework to break down a complex attack into minor stages, enabling analysts to tackle smaller problems simultaneously and helping the defenders implement separate controls for each phase. The cyber kill chain comprises seven stages: reconnaissance, weaponizing, delivery, exploitation, installation, command and control, and acting on objective [9]. Figure 2 illustrates the sequence of these stages.

Stage 1 – Reconnaissance**:** Information gathering (identification, selection, and profiling) about a potential target. The information gathered from reconnaissance is used in later stages of the cyber kill chain to design and deliver the payload. Reconnaissance is divided into two types: passive reconnaissance – gathering information about the target without letting him know about it; and active reconnaissance – deeper profiling of the target, which might trigger alerts.

Stage 2 – Weaponize: Backdoor designing and a penetration plan, utilizing the information gathered from reconnaissance. Technically, the backdoor binds software vulnerabilities with a remote access tool, creating a silent backdoor capable of evading user attention and security mechanisms.

Stage 3 – Delivery: Backdoor delivering, utilizing the information gathered from reconnaissance. Most deliveries require some kind of user interaction like downloading and executing malicious files or visiting malicious web pages on the Internet. Multiple delivery methods are used to increase the likelihood of delivery for delivering the weapon.

Stage 4 – Exploitation: After delivering the cyber weapon, the next step is triggering the exploit. The objective of an exploit is to install the payload silently. Certain conditions must be matched to trigger the exploit, such as the operating system and software versions and the ability to avoid anti-virus or other security mechanism detection. Multiple exploits increase the likelihood of exploitation for installing the payload.

Stage 5 – Installation: Malware nowadays is multi-staged and heavily relies on advanced techniques to deliver the malware modules in a sophisticated manner. Before executing the core code, the malware tries to disable host-based security controls to continue undetected. Additionally, instead of unpacking a large embedded copy of the core malware agent, some malware is connected to a remote file repository to download the core components.

Stage 6 – Command and Control**:** Command and Control (C&C) systems give remote instructions to compromised machines. C&C systems can be centralized, peer-to-peer decentralized, or rely on a social network. Today's malware use techniques to hide communication patterns with its C&C. Anonymous communication techniques involve creating a channel resistant to traffic analysis, such as hiding data inside media, using the TOR network, using encrypted channels, etc.

Stage 7 – Act on the objective: After getting the communication set up with the target system, the attacker executes the remote instructions based on its objective. This is an elaborate active attack process that takes months.

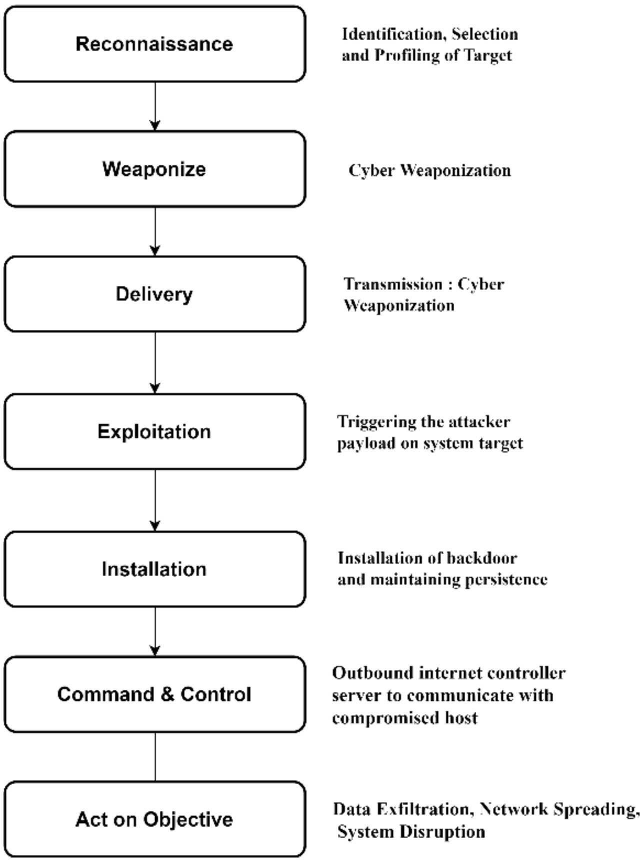

Reconnaissance
Identification, Selection and Profiling of Target
Weaponize
Cyber Weaponization
Delivery
Transmission : Cyber Weaponization
Exploitation
Triggering the attacker payload on system target
Installation
Installation of backdoor and maintaining persistence
Command & Control
Outbound internet controller server to communicate with compromised host
Act on Objective
Data Exfiltration, Network Spreading, System Disruption

Figure 2: Phases of Cyber Kill Chain, adapted from [9]

1.4 Pyramid of Pain (POP)

Pyramid of Pain (POP) is a cyber threat defender model and threat hunting framework. This model describes the efficacy of several indicators, such as Hash values, IP addresses, DNS, Network artifacts, Host artifacts, Tools, and TTPs, and places them at different levels of the pyramid according to their importance, as shown in Figure 3. It emphasizes that addressing low-level CTI data such as hash values, IPs, and DNS will cause minor damage to the adversary while working on high-level CTI data such TTPs makes organizations one step ahead of the attacker. Pyramid of pain elaborates on the importance of TTP in defending organizational security architecture.

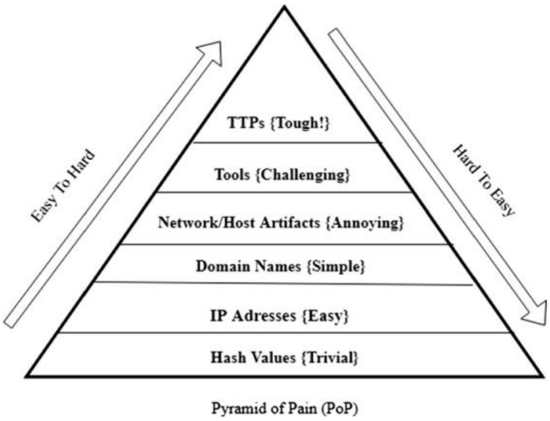


Figure 3: Pyramid of Pain (POP)

2. Literature Review

Cyber security has become a matter of global interest, and several attacks target industrial Companies and governmental organizations. Advanced persistent threats (APTs) have emerged as a new and complex version of multistage attacks (MSAs) targeting selected companies and organizations. Current APT detection systems focus on raising the detection alerts rather than predicting TTPs used in APTs. Predicting the TTPs at APT stages reveals the APT life cycle in its early stages and helps to understand the attacker's strategies and aims. Security is challenging due to the inherent vulnerabilities and threats from any part of the Network that can be exploited. This can cause severe disruption to the overall business continuity. Therefore, it is paramount to understand and predicate the threats so that the

Organizations can undertake necessary control measures. Cyber Threat Intelligence (CTI) provides intelligence analysis to discover unknown to known threats using various properties, including threat actor skill and motivation, Tactics, Techniques, Procedure (TTP), and Indicator of Compromise (IoC).

Zhou et al. [17] proposed a method to automatically identify Indicators of Compromise (IOC), an essential artifact of cyber threat intelligence, using a Neural-Based sequence labelling model to identify IOCs from CTRs. The model used an attention mechanism and token spelling features to identify low-frequency IOCs from long sentences of the cybersecurity reports. At the same time, our focus is to identify the adversarial techniques TTPs that can exploit the specific threat. The low-level IOCs mainly comprise volatile data and could be fabricated through fake threat intelligence, feeds, or events. The MITRE ATT&CK Framework provides a rich and actionable repository of adversarial tactics, techniques, and procedures (TTP). However, this information would be beneficial for attack diagnosis (i.e., forensics) and mitigation (i.e., intrusion response) if we can reliably construct technique associations that predict unobserved attack techniques based on observed ones. Al-Shaer [15] et al. presented statistical machine learning analysis on Advanced Persistent Threat (APT) reported by MITRE ATT&CK to infer and predict the techniques the adversary might use. They associated adversarial techniques using hierarchical clustering with 95% confidence.

In comparison, our focus is to automatically correlate individual threat information available in CTRs to the adversarial techniques provided by MITRE and create a model that can be used to map novel threats to the MITRE ATT&CK framework. Software vulnerabilities are the root causes of various security risks. Once malicious attacks exploit a vulnerability, it will significantly compromise the system's safety and may even cause catastrophic losses. Hence automatic classification methods are desirable to effectively manage the vulnerability in software, improve the security performance of the system, and reduce the risk of the system being attacked and damaged. There have also been works on classifying the vulnerability information based on its textual description. Huang et al. [19] proposed an automatic vulnerability classification model built on Term Frequency- Inverse Document Frequency (TFIDF), Information Gain (IG), and a deep neural network [9]. They validated their model with CVE descriptions of the National Vulnerability Database and compared them to the performances of SVM, Naive Bayes, and KNN algorithms. We attempt to classify the threat actor's tactical information based on its textual description. Still, Huang et al. [19] focused on a multi-class classification where each vulnerability belongs to a specific category. In contrast, we attempt to classify TTPs or threat information simultaneously into multiple adversarial techniques and generate an output in compliance with STIX.

References	Type & Year	Impact Factor	Core Objective	Classification Methods	Evaluation Matrix	CTI	TTPs	Accuracy
[11]	Journal (2021)	2.074	Cyber Security Threat Modeling : MITRE ATT&CK	NLP	-	Yes	Yes	-
[12]	Journal (2021)	8.038	CTI Knowledge Graph	Named Entity Recognizer (NER)	Recall, Precision	Yes	Yes	Recall Rate: 79% Precision: 80%
[13]	Journal(2021)	2.1	Map: Cyber Threats on MITRE ATT&CK	Multi-Label Classification	Accuracy	Yes	Yes	86%
[14]	Journal (2020)	7.18	SCREM : Framework for Cyber Threat Sharing (STIX 2.0)	Mathematical Model	-	Yes	Yes	-
[15]	Journal (2019)	7	Retrieving Cyber Threat Attributes from CTRs	Distributional Semantic Technique	Accuracy, Precision	Yes	Yes	Accuracy: 94% Precision: 33%
[16]	Journal (2021)	1.79	Extracting Threat Actions from Cyber Threat Intelligence Report	Decision Tree, RF, SVM, LR, MLPC	Recall Rate, Precision	Yes	Yes	Recall Rate: 82.24 Precision: 89.19

Table 1: Comparative analysis of relevant research

Hemberg et al. proposed an open-source, relational graphing tool, BRON, which links MITRE ATT&CK, CWE, CAPEC, and CVE information to gain further insight from available threat intelligence [10]. Threat data from MITRE ATT&CK, CAPEC, CWE, CVE, MITRE Engage, and MITRE D3FEND data sources are linked in a BRON graph. The data types are linked with bidirectional edges. Their proposed method correlated those publicly accessible information sources to make it more usable for the analysts and systematically hunt the threat. Our approach is similar by associating the available threat information with a publicly accessible knowledge base of MITRE ATT&CK to assist the human analysts.

3. Problem Analysis

The collection and organization of technical knowledge that can detect, evade, or mitigate cyber-attacks is known as cyber threat intelligence (CTI). That knowledge might be tactical (describing an attacker's technique, tools, and tactics utilized during an attack) or technical (comprising mostly indicators of compromise IOCs only).

Technical threat information – i.e., domain names, IP addresses, file hashes, etc. (low-level IOCs) – is comparatively easy to collect. This is due to the availability of numerous tools that can extract low-level IOCs from CTI. Unfortunately, this is not the case with tactical threat information (i.e., TTPs). Tactical threat information is highly challenging to retrieve and has significant value. Understanding the adversaries' tactics is highly critical and assists cyber security specialists to construct a better defense against the emerging cyber threats, which means adversaries must waste more resources to intrude into the target network.

In the same way, the data produced in both cases might be structured (for example, IP blacklists) or unstructured (e.g., CTRs). Specifically, the unstructured data requires manual analysis or natural language processing (NLP) techniques to extract the most critical information. As a result, obtaining vital tactical information from CTRs is quite difficult. Due to the unavailability of relevant tools, security specialists must now read and mine information from CTRs manually. The manual analysis of the reports is time-consuming and expensive. Subsequently, evaluating the number of CTRs published daily is a cumbersome task for security analysts. Therefore, security experts look forward to automating the extraction of tactical information TTPs from CTRs in a structured format, which they could use more efficiently.

4. Problem Statement

Tactical Intelligence is a high-level intelligence. The only authentic sources of tactical intelligence is Cyber Threat Reports (CTRs) that are published by resilient cyber security platforms. These CTRs help security analysts to understand upcoming threats and define countermeasure against emerging adversaries. If security analysts understand the tactics and techniques of threat actors, the countermeasure would be more accurate and effective. Due to the large volume of CTRs being launched daily from Cyber Security companies, it is quite a tough job for an analyst to read and extract TTPs from reports. This thesis aims to automate this procedure of extracting TTPs and sharing them globally through open-source platforms like MISP and OpenCTI.

5. Research Objective

We can summarize our research objective in one research question: ***How can we retrieve/extract high-level indicators of compromise (TTPs) from unstructured sources of cyber threat intelligence (i.e., CTRs)?*** Moreover, based on this research question, we address the following sub objectives:

1) Perform comparative analysis of novel NLP classifiers (BERT, RoBERTa , XLNet).

2) How can we solve the imbalanced dataset problem to improve the classification?

3) Map Techniques, Tactics & Procedures (TTPs) on MITRE framework.

6. Research Scope & Limitation

The thesis anticipates that the proposed solution will be used primarily on short reports only (daily, monthly) about a specific threats, rather than more in-depth annual reports containing descriptions of multiple threats at once.

7. Significance of the study

Firstly, the unstructured form of cyber threat information (i.e., cyber threat reports (CTRs)) contain high-level indicators of compromises (that are the techniques used by the adversaries to launch a cyber-attack). These techniques are of significant worth because, the CTRs are published by well-established cyber firms with decades of research and development in the field of cyber security. The huge number of cyber threat reports are published on monthly, quarterly and annually basis. These reports are analyzed and understood manually by cyber security analyst, which is a quite hectic job in this era of emerging AI and ML platforms. This thesis aims to find best NLP algorithm with high accuracy so that the whole process of manual report analysis can be automated. Time and energy spent by cyber security professionals and firms would be reduced because to this automation.

8. Proposed Methodology

The core task of the proposed model is to extract high-level indicators ofcompromises (IOCs) from unstructured sources of cyber threat intelligence (CTI). In order to fulfil this Objective MITRE ATT&CK dataset (consisting of 2000 + published CTI Reports from 2014 to 2021) is to be used in the training machine learning model. The dataset is labelled and structured in STIX 2.0 format (Structured Threat Information Expression). In the evaluation and testing phase, the unlabeled CTR can be separated into two types: the ones written in HTML and the other ones in PDF format. The TTPs from the document in PDF format can easily be extracted using the proposed model. However, the ones in HTML are more challenging to extract, as they are not all from the same source. Around Five hundred different websites host CTRs, which means that there are multiple HTML architectures exist. To simplify the extraction, the model parsed only the text in paragraph HTML tags and manually copied the reports, which could not be collected this way. The noises in the report could hinder the classification. This problem would be solved during the pre-processing phase of the text. The extracted TTPs from CTRs are then converted into STIX 2.0 format and published on public/open-source cyber threat platforms such as MISP & Open CTI.

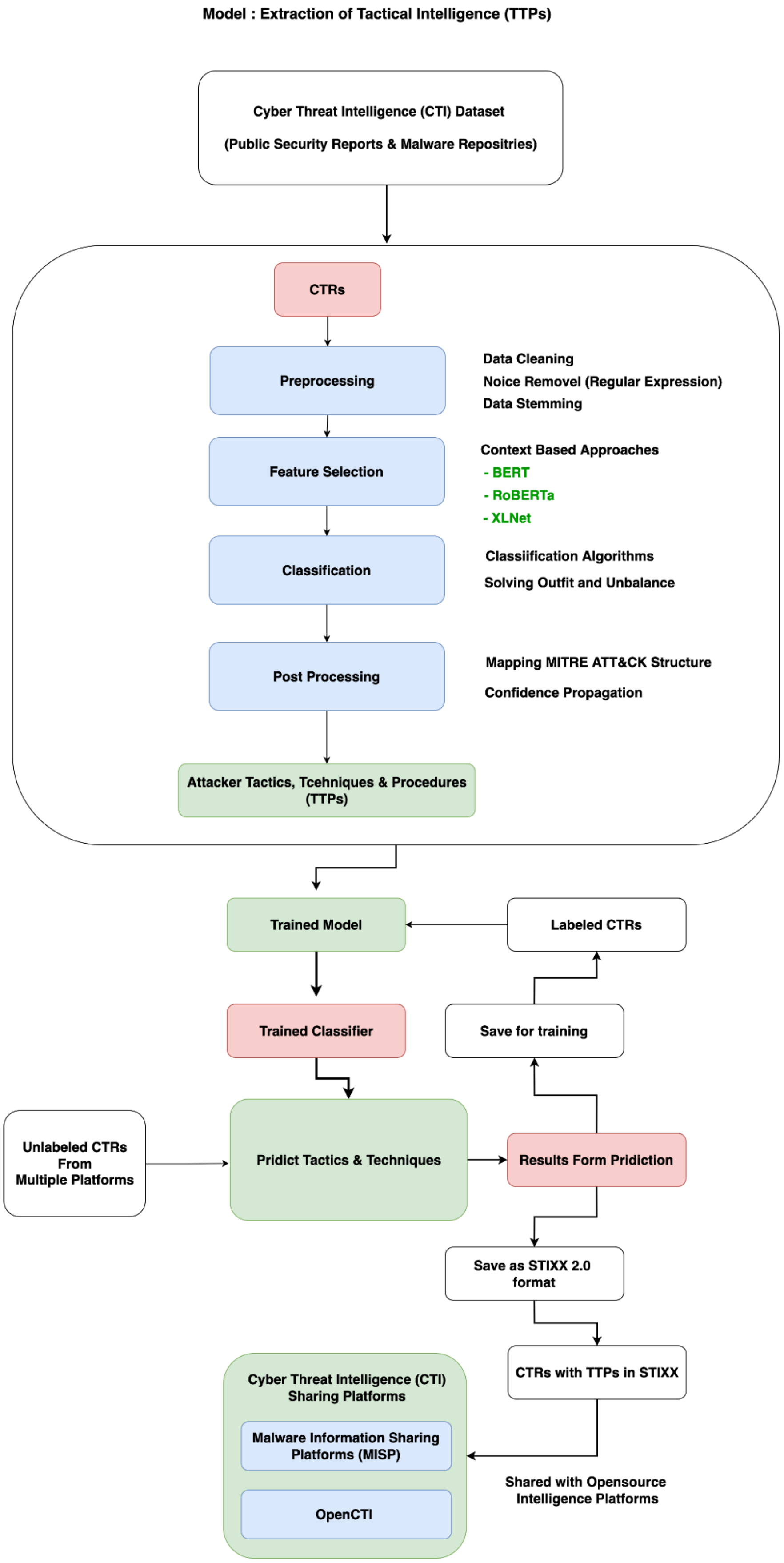
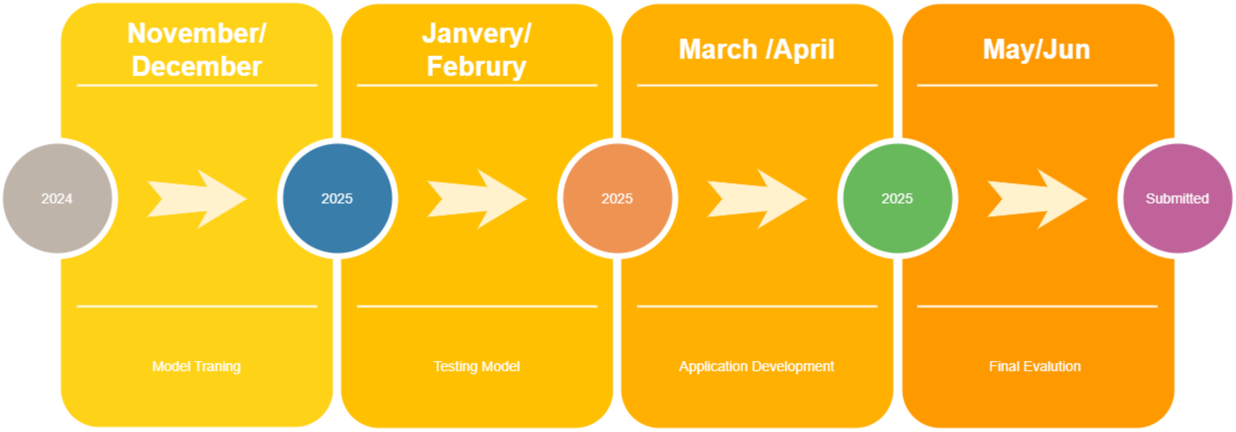

Model : Extraction of Tactical Intelligence (TTPs)
Cyber Threat Intelligence (CTI) Dataset
(Public Security Reports & Malware Repositries)
CTRs
Preprocessing
Data Cleaning
Noice Removel (Regular Expression)
Data Stemming
Feature Selection
Context Based Approaches
- BERT
- RoBERTa
- XLNet
Classification
Classiification Algorithms
Solving Outfit and Unbalance
Post Processing
Mapping MITRE ATT&CK Structure
Confidence Propagation
Attacker Tactics, Tcehniques & Procedures (TTPs)
Trained Model
Labeled CTRs
Trained Classifier
Save for training
Unlabeled CTRs From Multiple Platforms
Pridict Tactics & Techniques
Results Form Pridiction
Save as STIXX 2.0 format
CTRs with TTPs in STIXX
Cyber Threat Intelligence (CTI) Sharing Platforms
Malware Information Sharing Platforms (MISP)
OpenCTI
Shared with Opensource Intelligence Platforms

Figure 4: Model for extraction of TTPs from CTRs

4. Timeline


November/ December
Janvery/ Februry
March /April
May/Jun
2024
2025
2025
2025
Submitted
Model Traning
Testing Model
Application Development
Final Evalution

References

[1] Recorded Future. (2019). Understand Your Attacker: A Practical Guide to Identifying TTPs With Threat Intelligence. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/white-papers/identifying-ttps.pdf

[2] Bromander, V. M. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). Athens, Greece: EISIC

[3] The MITRE Corporation. (2017). FINDING CYBER THREATS WITH ATT&CK-BASED ANALYTICS. Whitepaper, McLean, VA. Retrieved December 7, 2020

[4] David Bianco. A framework for cyber threat hunting part 1: The pyramid of pain, 2015.

[5] Xiaoli Lin, Pavol Zavarsky, Ron Ruhl, and Dale Lindskog. Threat modelling for csrf attacks. 2013 IEEE 16th International Conference on Computational Science and Engineering, 3:486–491, 2009.

[6] BSM. Attack models with bsimm frameworks. Online, https://www.bsimm.com/framework/intelligence/attack-models/, 2016.

[7] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso. Cyber-attack modelling analysis techniques: An overview. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 69–76, Aug 2016.

[8] Tolulope Awojana. Threat modelling and analysis of web application attacks. 2018.

[9] W. Tounsi e H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," 2018. Available:https://www.researchgate.net/publication/320027747_A_survey_on_technical_threat_intelligence_in_the_age_of_sophisticated_cyber_attacks.

[10] FireEye Inc., "Taking a Lean-Forward Approach to Combat Today's Cyber Attacks," 2014. [Online].

[11] P. Chen, L. Desmet e C. Huygens, "A Study on Advanced Persistent Threats," 2016. [Online]. Available: https://hal.inria.fr/hal-01404186/document.

[12] 11Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modelling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177.

[13] Sarhan, I., & Spruit, M. (2021). Open-cykg: An open cyber threat intelligence knowledge graph. *Knowledge-Based Systems*, *233*, 107524.

[14] Mendsaikhan, O., Hasegawa, H., Yamaguchi, Y., & Shimada, H. (2020). Automatic mapping of vulnerability information to adversary techniques. *The Fourteenth International Conference on Emerging Security Information, Systems and Technologies SECUREWARE2020*.

[15] Ramsdale, Andrew, Shiaeles.S, and Kolokotronis.N. 2020a. "A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats, and Languages." Electronics (Switzerland) 9(5).

[16] Zhang, H., Shen, G., Guo, C., Cui, Y., & Jiang, C. (2021). EX-Action: Automatically Extracting Threat Actions from Cyber Threat Intelligence Report Based on Multimodal Learning. Security and Communication Networks, 2021.

[17] Al-Shaer, R., Spring, J. M., & Christou, E. (2020, June). Learning the associations of mitre att & CK adversarial techniques. 2020 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.

[18] Yang, W., & Lam, K. Y. (2019, December). Automated cyber threat intelligence reports classification for early warning of cyber attacks in next-generation SOC. International Conference on Information and Communications Security (pp. 145-164). Springer, Cham.

[19] Zhou, S., Long, Z., Tan, L., & Guo, H. (2018). Automatic identification of indicators of compromise using neural-based sequence labelling. arXiv preprint arXiv:1810.10156.

[20] Husari, G., Niu, X., Chu, B., & Al-Shaer, E. (2018, November). Using entropy and mutual information to extract threat actions from cyber threat intelligence. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE.

[21] Huang, G., Li, Y., Wang, Q., Ren, J., Cheng, Y., & Zhao, X. (2019). Automatic classification method for software vulnerability based on deep neural Network. IEEE Access, 7, 28291-28298.

[22] Hemberg, E., Kelly, J., Shlapentokh-Rothman, M., Reinstadler, B., Xu, K., Rutar, N., & O'Reilly, U. M. (2020). Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting. arXiv preprint arXiv:2010.00533.